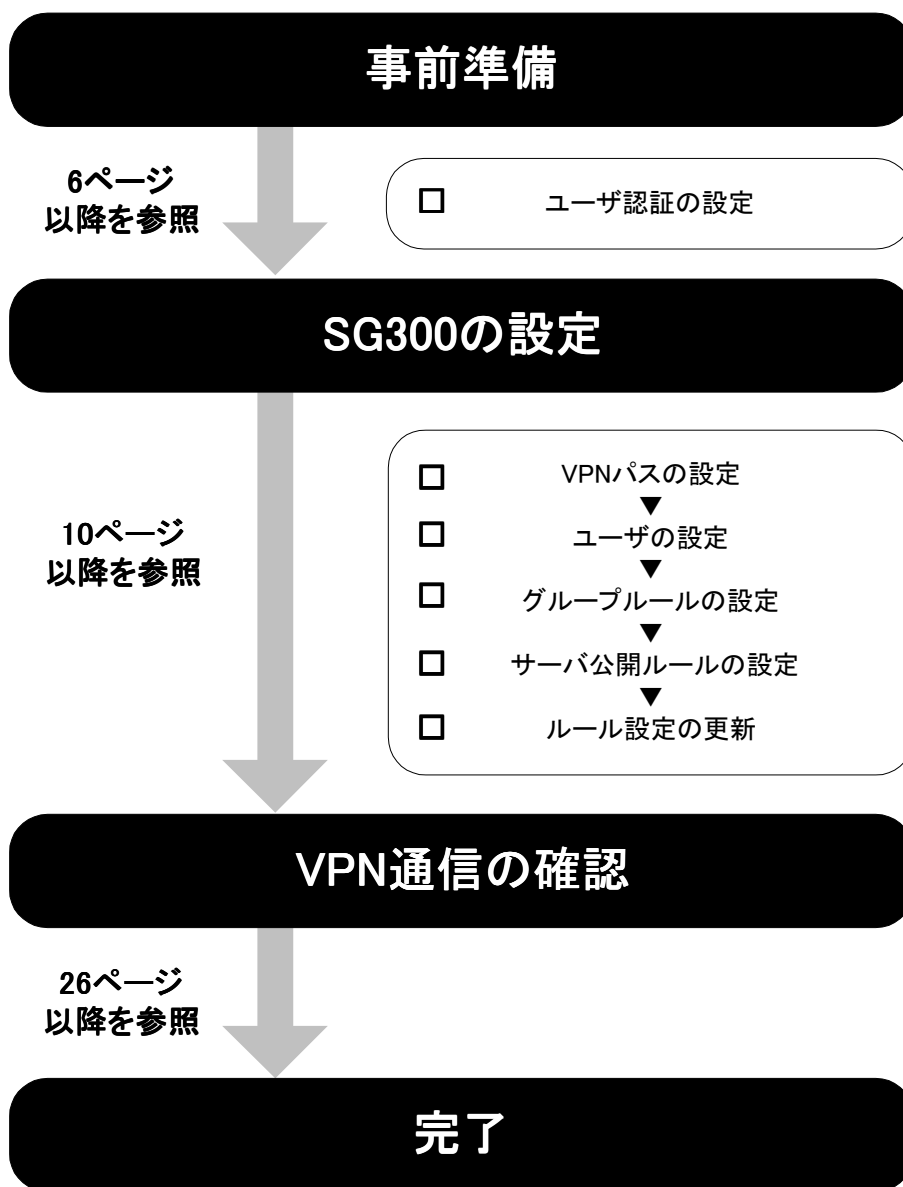
2 VPNサーバの設定

本章では、SG300側で行うリモートアクセスVPNの設定について、順番に説明します。

作業の流れ

リモートアクセスVPN環境を構築する場合、SG300側では図のような流れで作業を行います。

事前準備

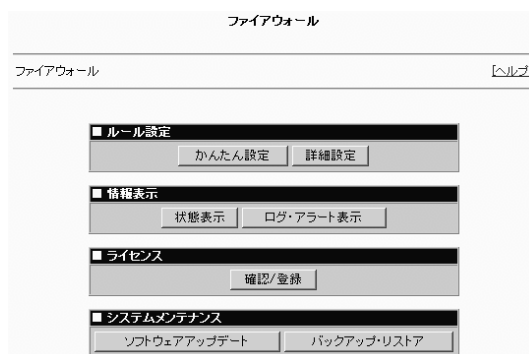
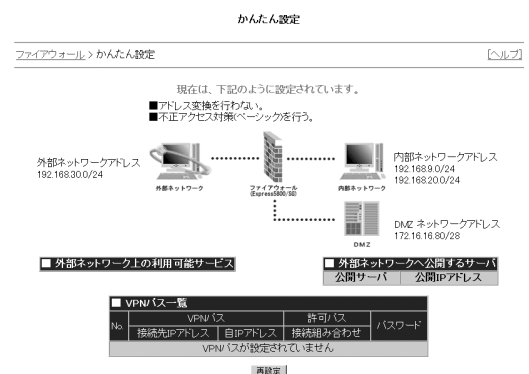
リモートアクセスVPN環境を構築するには、ユーザ認証が必須となります。そのため、VPN設定前の事前準備として、かんたん設定でユーザ認証が利用できるように設定しておく必要があります。

本書では、リモートアクセスVPNを利用するユーザをuser_tokyoとし、ユーザ(user_tokyo)が所属するグループをvpn_groupとしています。
ユーザの設定の詳細はP14「ユーザの設定」を参照してください。

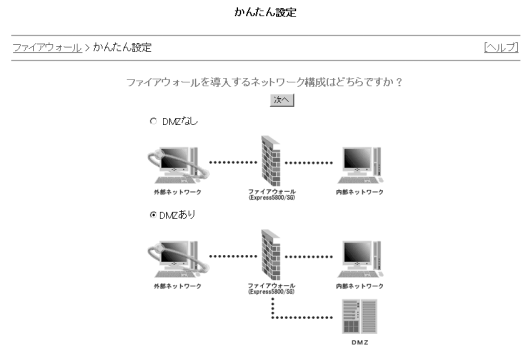
ユーザ認証の設定

かんたん設定でユーザ認証を利用可能にします。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアーウォール]をクリックする。
   ファイアウォールメニュー画面が表示されます。

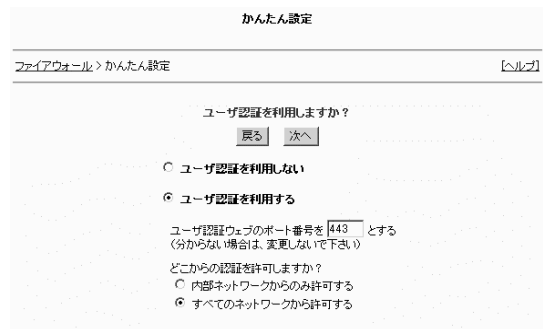
2. ファイアウォールメニューの「ルール設定」から[かんたん設定]をクリックする。
   設定内容確認画面が表示されます。

3. [再設定]をクリックする。
   ネットワークの構成の選択画面が表示されます。

4. [次へ]をクリックする。

同様にユーザ認証の利用選択画面が表示されるまで、[次へ]をクリックする。

ユーザ認証の利用選択画面が表示されます。

ネットワークの構成選択画面からユーザ認証の利用選択画面までの遷移は以下のとおりです。

ネットワークの構成選択画面→インタフェース選択画面→ウェブサーバ公開の設定画面→メールサーバ公開の設定画面→ファイル転送サーバ公開の設定画面→ネームサーバ公開の設定画面→その他の公開サーバの設定画面→外部ネットワーク利用サービス選択の画面→より強固な不正アクセス対策の設定画面→ユーザ認証の利用選択画面

5. 「ユーザ認証を利用する」のラジオボタンと「すべてのネットワークから許可する」のラジオボタンを選択し、[次へ]をクリックする。

VPN利用選択画面が表示されます。

6. [設定の確認へ]をクリックする。

設定内容確認画面が表示されます。

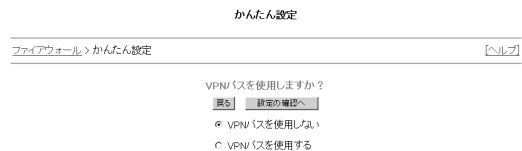
かんたん設定

ファイアウォール > かんたん設定 [ヘルプ]

VPNパスを使用しますか？

戻る 設定の確認へ

VPNパスを使用しない

VPNパスを使用する

7. [設定]をクリックする。

ルール適用画面が表示されます。

8. [かんたん設定を終了]をクリックする。

ファイアウォールメニュー画面に戻ります。

9. 以上で、事前準備は終了しました。

SG300の設定

リモートアクセスVPN環境を構築するためには、SG300(tokyo)側で以下の項目を設定しておく必要があります。

●VPNパスの設定

●ユーザ設定

●グループルールの設定

●サーバ公開ルールの設定

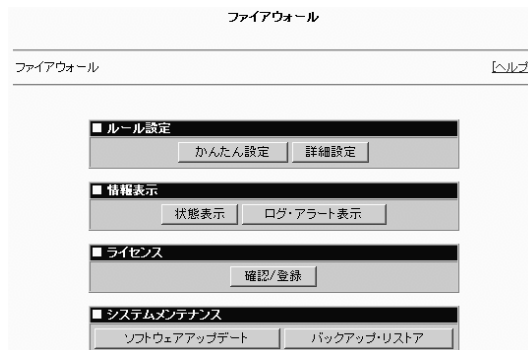
VPNパスの設定

VPN環境を構築するためには、まずは、VPNパス（自動鍵交換：トランスポートモード）の設定を行います。

1．Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアーウォール]をクリックする。

ファイアウォールメニュー画面が表示されます。

2．ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

詳細設定メニュー画面が表示されます。

3．詳細設定メニューの「VPN設定」から[VPNパス設定]をクリックする。

VPN情報一覧画面が表示されます。

4. 「一覧の末尾にVPNパス（自動鍵交換：トランスポートモード）を『追加』」をクリックする。
VPNパス追加画面（自動鍵）が表示されます。

5. VPNパス追加画面（自動鍵）に表示される各項目を設定する。

	項目	設定内容
VPNパス	接続先IPアドレス	202.247.5.0/24
	自IPアドレス	202.247.5.136
	暗号化／認証	AES128 & MD5
	有効期間	3600
	共有秘密鍵	パスワード（プリシェアードシークレット）
	暗号化／認証（AH）	チェックしない
	暗号化／認証（ESP:暗号アルゴリズム）	AES128
	暗号化／認証（ESP:認証アルゴリズム）	HMAC MD5
	鍵の有効期間	28800
オプション	PFS（Perfect Forward Secrecy）の有効	チェックする
	IPSecで鍵更新を行う	チェックする

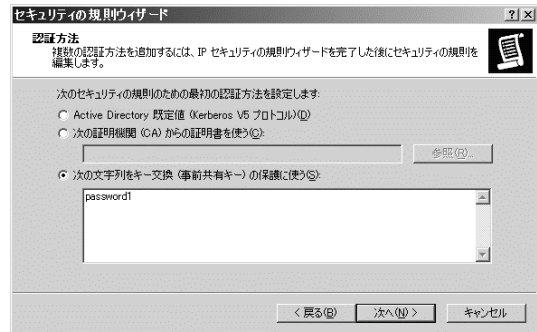
接続先IPアドレスにはクライアント側のネットワークアドレスを指定します。

共有秘密鍵でパスワードを選択した場合、クライアントのパスワードと同じ文字列でなければなりません。

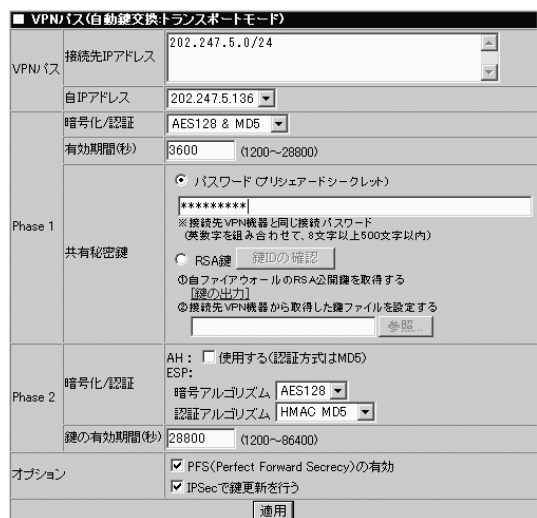
WIndows XP（クライアント側）では、セキュリティ規則作成時の「認証方法」でパスワードを設定します。

パスワードは必ず英数字を組み合わせて、8文字以上500文字以内で入力します。

（右記の例では「password1」と記しています。）

設定の詳細は『リモートアクセスVPNの設定（クライアント編）』P10「セキュリティ規則の作成」手順12を参照してください。

以上の設定項目はP4「VPN構築の前提条件」にあわせた一例として説明しています。接続先IPアドレス、自IPアドレス等は、適宜お客様の環境にあわせて設定してください。

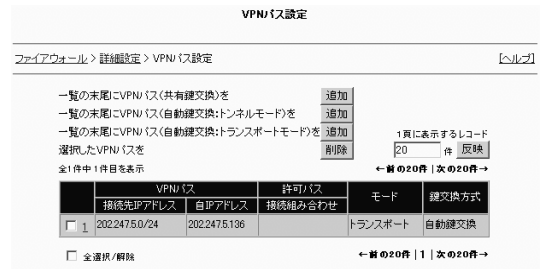
6. [適用]をクリックする。

   VPNパス登録結果画面（自動鍵）が表示されます。

7. [VPNパス設定に戻る]をクリックする。

追加したVPNパスが反映されたVPNパス設定画面が表示されます。

8. 追加したVPNパスが反映されていることを確認し、[詳細設定]をクリックする。

詳細設定メニュー画面が表示されます。

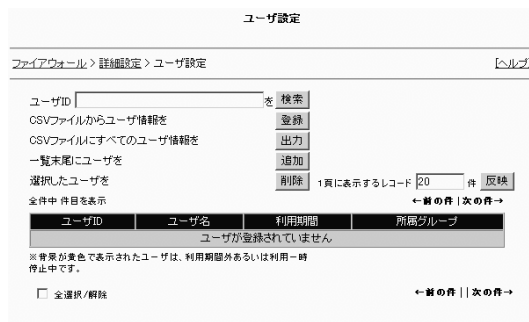
引き続きユーザの設定を行います。

ユーザの設定

ユーザの作成、所属するグループの登録の各設定を行います。

ユーザの作成

ユーザの作成を行います。

1．詳細設定メニューの「ユーザ設定」から[ユーザ設定]をクリックする。
ユーザ情報一覧画面が表示されます。

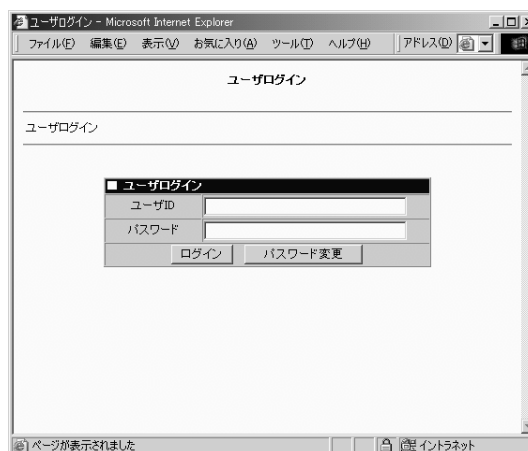
2．「一覧末尾にユーザを『追加』」をクリックする。
ユーザ情報登録画面が表示されます。

3．ユーザ情報登録画面に表示される各項目を設定する。

項目	設定内容
ユーザ名	user_tokyo
ユーザID	user_tokyo
パスワード	6文字から256文字までの英数文字列
再パスワード	（上記と同じ文字列を入力）
備考	（空白）
利用期間	（任意の期間を指定）

項目	設定内容
利用を一時停止する	チェックしない

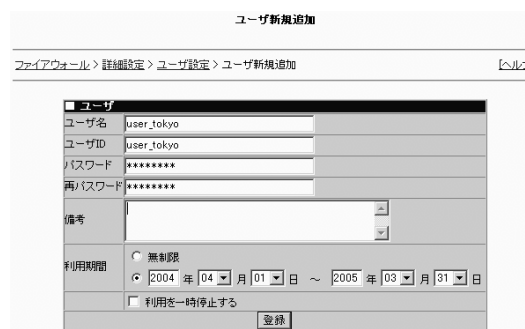
クライアント（Windows XP側）がインターネット経由で企業内ネットワークへアクセスする場合、まず、「ユーザログイン」が表示され、本項目で設定したユーザIDとパスワードの入力が必要になります。

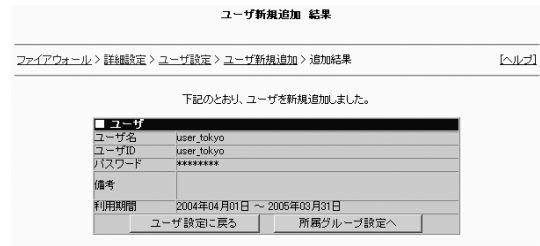
本書では、リモートアクセスVPNを利用するユーザIDを「user_tokyo」とし、パスワードは英数文字列で6文字以上256文字以内としています。

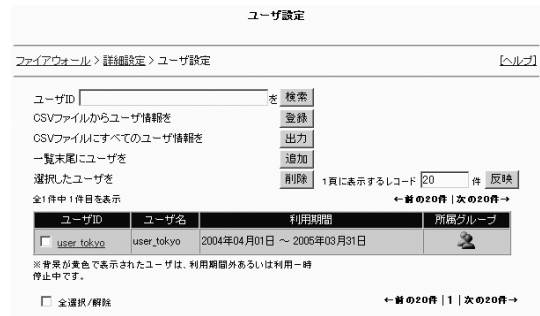
詳細は『リモートアクセスVPNの設定（クライアント編）』P19「ユーザ認証」手順2を参照してください。

4. [登録]をクリックする。

ユーザ情報登録結果画面が表示されます。

2

VPNサーバの設定

5. ユーザ情報登録結果画面の[ユーザ設定に戻る]をクリックする。

ユーザ情報一覧画面に戻ります。新しく登録されたユーザ情報が一覧に反映された形で表示されます。

6. ユーザ情報一覧画面を確認し、[詳細設定]をクリックする。

詳細設定メニュー画面が表示されます。引き続きユーザの設定（グループの作成）を行います。

グループの作成

ここでは、グループの作成を行います。

7. 詳細設定メニューの「ユーザ設定」から[グループ設定]をクリックする。

グループ情報一覧画面が表示されます。

8. 「一覧末尾にグループを『追加』」をクリックする。

グループ情報登録画面が表示されます。

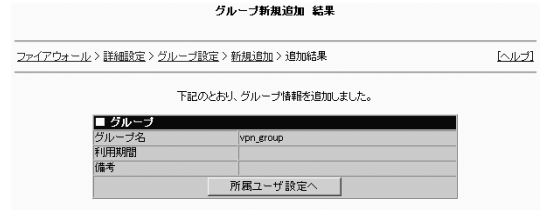
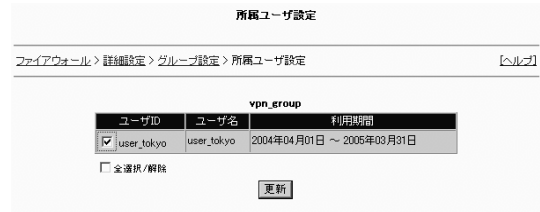
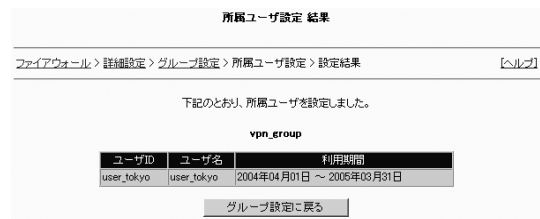
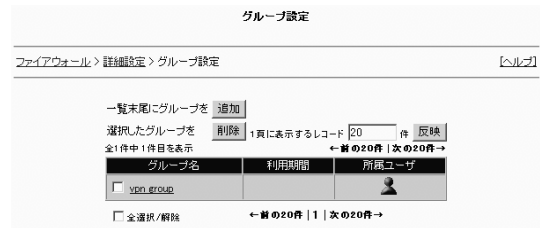
9. グループ情報登録画面に表示される各項目を入力する。

項目	設定内容
グループ名	vpn_group
利用期間	任意の期間を指定
備考	（空白）

本書では、リモートアクセスVPNを利用するユーザをuser_tokyoとし、ユーザ(user_tokyo)が所属するグループをvpn_groupとしています。

10. [登録]をクリックする。

グループ情報登録結果画面が表示されます。

１１．［所属ユーザ設定へ］をクリックする。
所属ユーザ選択画面が表示されます。

１２．先ほど作成したユーザ（user_tokyo）のチェックボックスをチェックし、［更新］をクリックする。
所属ユーザ登録結果画面が表示されます。

１３．［グループ設定に戻る］をクリックする。
グループ情報一覧画面に戻ります。新しく登録されたグループ情報が一覧に反映された形で表示されます。

１４．グループ情報一覧画面を確認し、［詳細設定］をクリックする。
詳細設定メニュー画面が表示されます。
引き続きグループルールの作成を行います。

グループルールの設定

グループルールを作成します。

1．詳細設定メニューの「ルール設定」から[グループ設定]をクリックする。

グループ情報一覧画面が表示されます。

2．「一覧末尾にグループルールを『追加』」をクリックする。

グループ選択画面が表示されます。

3．ルールを追加するグループ名（vpn_group）のラジオボタンをクリックし、「選択したグループのグループルールを『追加』」をクリックする。

選択したグループのルール一覧画面が表示されます。

4．「一覧末尾に『追加』」をクリックする。

個別ルール追加画面が表示されます。

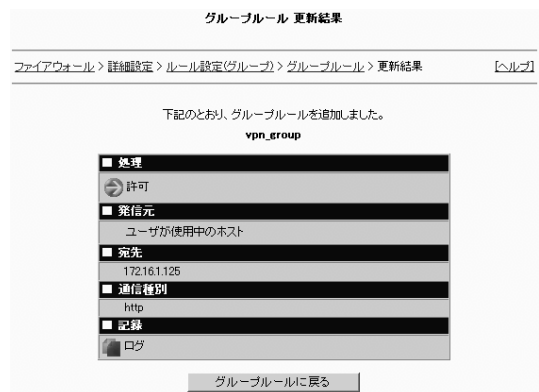
5. 個別ルール追加画面に表示される各項目を設定する。

項目	設定内容
宛先	ユーザ指定（ラジオボタン）、172.16.1.125（テキストボックス）
通信種別	ユーザ指定（ラジオボタン）、http（テキストボックス）
記録	ログ

6. ［登録］をクリックする。

個別ルール追加画面が表示されます。

7. ［グループルールに戻る］をクリックする。

追加したルールが反映された、選択したグループのルール一覧画面が表示されます。

8. 「トランスポートVPNパスを『変更』」をクリックする。

トランスポートVPNパス選択画面が表示されます。

９． 表示されるトランスポートVPNパスの中から先ほど設定したVPNパスのチェックボックスをチェックし、[登録]をクリックする。

選択したグループルールの一覧画面に戻ります。

トランスポートVPNパス選択

ファイアウォール > 詳細設定 > ルール設定(グループ) > グループルール > トランスポートVPNパス選択 [ヘルプ]

グループルールに登録するトランスポートVPNパスを選択してください。

	VPNパス		モード	鍵交換方式
	接続先IPアドレス	自IPアドレス		
☑ 1	202.247.5.0/24	202.247.5.136	トランスポートモード	自動鍵

☐ 全選択/解除

登録

項目	チェック内容
接続先IPアドレス	202.247.5.0/24
自IPアドレス	202.247.5.136
モード	トランスポートモード
鍵交換方式	自動鍵

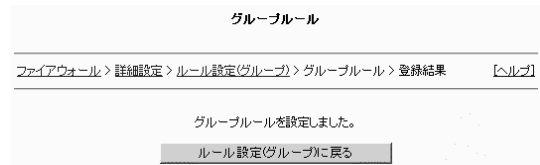
１０． 「認証有効時間」のテキストボックスに、ユーザ認証の後、ルールを有効にしておく時間を入力する。

（右記の例では60[分]としています。）

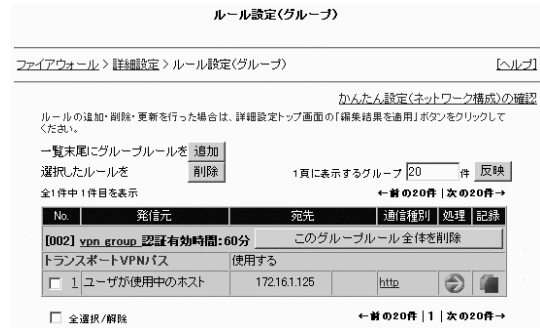
１１． [登録]をクリックする。

グループルール登録結果画面が表示されます。

１２． [ルール設定（グループ）に戻る]をクリックする。

グループ情報一覧画面が表示されます。

１３． グループ情報一覧画面を確認し、[詳細設定]をクリックする。

詳細設定メニュー画面が表示されます。

引き続きサーバ公開ルールの設定を行います。

サーバ公開ルールの設定

サーバ公開ルールを作成します。

1． 詳細設定メニューの「ルール設定」から[サーバ公開ルール]をクリックする。

サーバ公開ルール一覧画面が表示されます。

2． 「一覧末尾にルールを『追加』」をクリックする。

サーバ公開ルール追加画面が表示されます。

3． サーバ公開ルール追加画面に表示される各項目を設定する。

項目	設定内容
外部公開IPアドレス	202.247.5.136
内部IPアドレス	172.16.1.125
ポート	TCP（外部80→内部80）
記録	ログ

4. [登録]をクリックする。

サーバ公開ルール登録結果画面が表示されます。

5. [ルール設定（サーバ公開）に戻る]をクリックする。

追加したルールが反映されたサーバ公開ルール一覧画面が表示されます。

6. サーバ公開ルール一覧画面を確認し、[詳細設定]をクリックする。

詳細設定メニュー画面が表示されます。

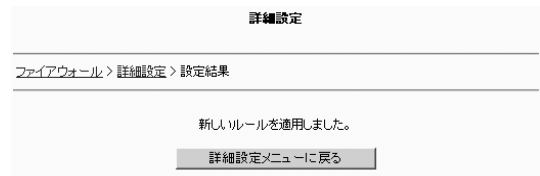
引き続きルール設定の更新を行います。

ルール設定の更新

最後に、今までの設定を更新します。

1. 詳細設定メニューの「ルール設定」から[編集結果を適用]をクリックする。

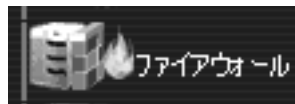
   詳細設定結果画面が表示されます。

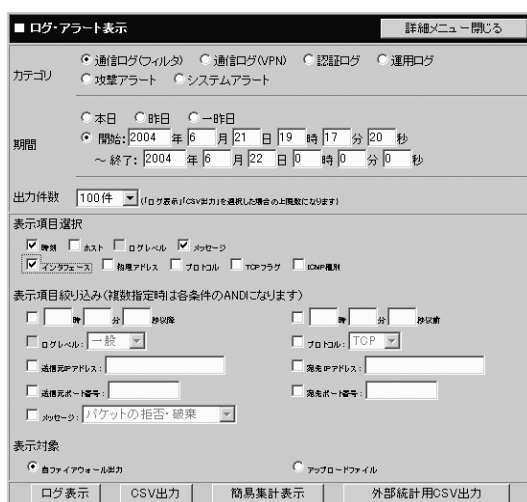
2. 新しく追加したルールがExpress5800/SG300に適用されます。

VPN通信の確認

ここでは、VPNパス間で暗号通信が正常に行えているかどうかを確認する方法について説明します。

VPNパス間で暗号通信ができているかどうかは、実際にVPNの対象となる通信を行った後、通信ログを参照することで確認します。確認手順を以下に示します。

VPNクライアントの設定の詳細は、「リモートアクセスVPNの設定（クライアント編）」を参照してください。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアーウォール]をクリックする。
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「情報表示」から[ログ・アラート表示]をクリックする。
   ログ・アラート表示画面が表示されます。

3. 「詳細メニュー開く」をクリックし、ログ・アラート表示画面に表示される各項目を入力する。

項目	設定内容
カテゴリ	通信ログ（フィルタ）
期間	VPNの対象となる通信を行った期間を指定
出力件数	（任意の件数を指定）
表示項目選択	時刻、メッセージ、インタフェース
表示項目絞り込み	VPNの対象となる通信を絞り込む条件を指定（特に指定しなくても可）
表示対象	自ファイアウォール出力

4. [ログ表示]をクリックする。

ログ表示画面が表示されます。右図の通り、VPN通信に該当するグループルールやサーバ公開ルールの出力の「入力I/F」欄に、ipsecという文字列が表示されていれば設定は成功です。

「入力I/F」欄にethという文字列が表示されている場合は、VPN通信が行われていません。再度、これまでの各設定を見直してください。

VPN通信に関するエラー情報は、ログ・アラート表示画面でカテゴリとして[通信ログ（VPN）]のラジオボタンを選択し、[ログ表示]をクリックすることで確認できます。